Written Statement of

Kevin J. Martin
Chairman
Federal Communications Commission

Hearing on
Phone Records For Sale:
Why Aren't Phone Records Safe From Pretexting?

Before the
Committee on Energy and Commerce
U.S. House of Representatives

February 1, 2006

Introduction

Good afternoon, Chairman Barton, Ranking Member Dingell, and members of the Committee. I appreciate the opportunity to speak with you today about what appears to be an alarming breach of the privacy of consumers' telephone records. The entire Commission is deeply concerned about the disclosure and sale of these personal telephone records and will take strong enforcement action to address any noncompliance by telecommunications carriers with the customer proprietary network information ("CPNI") obligations under section 222 of the Communications Act of 1934, as amended, (the Act) and the Commission's rules.

In my testimony, I will describe the Commission's current investigation into the procurement and sale of consumers' private phone records and the steps the FCC is taking to make sure that telecommunications carriers are fully meeting their obligations under the law to protect those records.

As the Committee is aware, the issue of third parties known as "data brokers" obtaining and selling consumers' telephone call records, which has been widely reported, is a tremendous concern for consumers, lawmakers, and regulators alike. Determining how this violation of consumers' privacy is happening and addressing it is a priority for the Commission. As outlined below, we are taking numerous steps to combat the problem. First, we are investigating the data brokers to determine how they are obtaining this information. Second, we are investigating the telecommunications carriers to determine whether they have implemented safeguards that are appropriate to secure the privacy of the personal and confidential data entrusted to them by American consumers. Third, we are initiating a proceeding to determine what additional rules the Commission

should adopt to further protect consumers' sensitive telephone record data from unauthorized disclosure.

Background

Numerous websites advertise the sale of personal telephone records for a price. Specifically, data brokers advertise the availability of cell phone records, which include calls to and/or from a particular cell phone number, the duration of such calls, and may even include the physical location of the cell phone. In addition to selling cell phone call records, many data brokers also claim to provide calling records for landline and voice over Internet protocol, as well as non-published phone numbers. In many cases, the data brokers claim to be able to provide this information within fairly quick time frames, ranging from a few hours to a few days.

The data brokers provide no explanation on their websites of how they are able to obtain such personal data.[1] There are several possible theories for how these data brokers are obtaining this information. These data brokers may be engaged in "pretexting," that is, obtaining the information under false pretenses – often by impersonating the account holder. In addition, they may be obtaining access to consumers' accounts online by overcoming carriers' data security protocols. To the extent this is the cause of the privacy breaches, we must determine whether this is in part due to the lack of adequate carrier safeguards. Finally, various telecommunications carriers could have "rogue" employees who are engaged in the practice of sharing this information with data brokers in exchange for a fee.

[1] The websites often contain statements that the information obtained is confidential and not admissible in court, and may specify that the purchaser must employ a legal avenue, such as a subpoena, for obtaining the

The mandate requiring telecommunications carriers to implement adequate safeguards to protect consumers' call records is found in section 222 of the Act. Congress enacted section 222 to protect consumers' privacy. Specifically, section 222 of the Act provides that telecommunications carriers must protect the confidentiality of customer proprietary network information. CPNI includes, among other things, customers' calling activities and history, and billing records. The Act limits carriers' abilities to use customer phone records even for their own marketing purposes without appropriate consumer approval and safeguards. Furthermore, the Act prohibits carriers from using, disclosing, or permitting access to this information without approval of the customer, or as otherwise required by law, if the use or disclosure is not in connection with the provided service.

When it originally implemented section 222, the Commission required telecommunications carriers to obtain express written, oral, or electronic consent from their customers, i.e., an "opt-in" requirement, before a carrier could use any customer phone records to market services outside the customer's existing service relationship with that carrier. The United States Court of Appeals for the Tenth Circuit (10th Circuit) struck down these rules finding that they violated the First and Fifth Amendments of the Constitution. Required by the 10th Circuit to reverse its "opt-in" rule, the Commission ultimately adopted an "opt-out" approach whereby a customer's phone records may be used by carriers, their affiliates, agents, and joint venture partners that provide communications-related services provided that a customer does not expressly withhold consent to such use.

---

data if the purchaser intends to use the information in a legal proceeding.

The Commission must determine whether carriers are complying with their obligations under section 222. In order to make this determination, we are examining the methods that data brokers use to gain access to consumers' call records, and the methods employed by carriers to guard against such breaches.

Commission Investigation

The issue of the disclosure and sale of consumer phone records was brought to the Commission's attention late last summer. On August 30th, the Electronic Privacy Information Center (EPIC) filed a petition for rulemaking expressing concern about the sufficiency of carrier privacy practices and the fact that online data brokers were selling consumers' private telephone data. At this same time, the Commission's Enforcement Bureau began researching and investigating the practices of data brokers. This research culminated in the Commission issuing subpoenas to several of the most prominent data broker companies. These subpoenas, served in November 2005, sought details regarding how the companies obtained this phone record information and contained further questions about the companies' sale of consumer call records. Unfortunately, the companies failed to adequately respond to our request. As a consequence, we issued letters of citation to these entities for failing to fully respond to a Commission order and referred the inadequate responses to the Department of Justice for enforcement of the subpoenas. In addition, we subsequently served another approximately 30 data broker companies with subpoenas and are currently waiting for their response. Finally, in support of these investigations, we have made undercover purchases of phone records from various data brokers. The purpose of this information is to assist us in targeting

additional subpoenas and in determining the exact method by which consumer phone record data is being disclosed.

In conjunction with our investigation of data brokers, the Commission also focused its attention on the practices of the telecommunications carriers subject to section 222. Specifically, in December and January, Commission staff met with the major wireless and wireline providers to discuss efforts they have undertaken to protect their confidential customer data and to prevent data brokers from obtaining and using such information. Discussions focused on the specific procedures employed to protect consumer call records from being accessed by anyone other than the consumers themselves. Staff also probed who within the companies has access to call record information and the procedures the carriers use to ensure that employees and other third parties with access to such information do not improperly disclose it to others. The carriers generally expressed their belief that the problems they have experienced in this area are largely, if not exclusively, related to attempts by individuals outside the company to obtain information through pretexting, rather than by "rogue" employees selling information to data brokers.

In order to have the carriers' responses in written form, last month, we sent formal Letters of Inquiry to these carriers. Inquiry letters are formal requests for information from carriers that may trigger penalties if not answered fully. These letters require the carriers to document their customer data security procedures and practices, identify security and disclosure problems, and address any changes they have made in response to the data broker issue.

In addition, under the Commission's rules, a telecommunications carrier "must have an officer, as an agent of the carrier, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that the company has established operating procedures that are adequate to ensure compliance" with the Commission's CPNI rules. In response to this Committee's letter, we asked the five largest wireline and wireless carriers to send us their CPNI certifications. Earlier this week, the Enforcement Bureau issued Notices of Apparent Liability in the amount of $100,000 against both AT&T and Alltel for failure to adequately respond to this request. We also issued a public notice requiring all telecommunications carriers to submit their most recent certification with us. To the extent that carriers are unable to do so, or do not respond adequately, we are prepared to take appropriate enforcement action against them as well.

Coordination with the FTC and State Attorneys General. Because this problem implicates the jurisdiction of both the FCC and FTC, we have coordinated with the FTC throughout our investigation. Beginning last summer, Commission staff and FTC staff have been in regular contact regarding the sale of phone records by data brokers. In addition, I met with Chairman Majoras late last year and discussed this issue, among others. Commission staff will continue to coordinate closely with the FTC staff and share with them any evidence of fraudulent behavior that we detect in the course of our investigation.

The FCC has also responded to several inquiries and provided guidance to individual state Attorneys General, and the National Association of Attorneys General (NAAG). As you are aware, a number of states, including Florida, Illinois, and Missouri have taken recent legal action against data brokers.

Commission's Efforts to Strengthen Existing CPNI Rules

As I mentioned previously, EPIC filed a petition with the Commission raising concerns about the sale of call records. Specifically, EPIC petitioned the Commission to open a proceeding to consider adopting stricter security standards to prevent carriers from releasing private consumer data. Several weeks ago, I circulated an item to my fellow Commissioners granting EPIC's petition and inviting comment on whether additional Commission rules are necessary to strengthen the safeguards for customer records. Specifically, we seek comment on EPIC's five proposals to address the unlawful and fraudulent release of CPNI: (1) consumer-set passwords; (2) audit trails; (3) encryption; (4) limiting data retention; and (5) notice procedures to the customer on release of CPNI data. In addition to these proposals, we also seek comment on whether carriers should be required to report further on the release of CPNI. Further, the item tentatively concludes that the Commission should require all telecommunications carriers to certify on a date certain each year that they have established operating procedures adequate to ensure compliance with the Commission's rules and file these certifications with the Commission.

This item has been distributed to the Commissioners for their consideration and will be acted on by February 10, 2006.

Legislative Assistance

In addition to the Commission's actions, several members have asked for the Commission's views on any potential changes to the law that could help combat this

troubling trend. There are three primary actions that I believe Congress could take to prevent data broker companies from selling consumers' phone records. First, I believe that Congress could specifically make illegal the commercial availability of consumers' phone records. Thus, if any entity is found to be selling this information for a fee, regardless of how it obtained such information, it would face liability.

Second, Congress could overturn the ruling of a federal court that limited the Commission's ability to implement more stringent protection of consumer phone record information. Specifically, when the Commission first implemented section 222, it required carriers to obtain express written, oral, or electronic consent from their customers, i.e., an "opt-in" requirement before a carrier could use any customer phone records to market services outside the customer's existing service relationship with that carrier. The Commission held that this "opt-in" requirement provided consumers with the most meaningful privacy protection. In August of 1999, the 10th Circuit struck down these rules finding that they violated the First and Fifth Amendments of the Constitution. Required by the 10th Circuit to reverse its "opt-in" rule, the Commission adopted an "opt-out" approach whereby a customer's phone records may be used by carriers, their affiliates, agents, and joint venture partners that provide communications-related services provided that a customer does not expressly withhold consent to such use. This ruling shifted the burden to consumers, requiring them to specifically request that their personal phone record information not be shared. This ruling has resulted in a much broader dissemination of consumer phone records and thereby may have contributed to the proliferation of the unlawful practices of data brokers that we are seeing today.

Third, I recommend that the Commission's enforcement tools be strengthened. For example, the need to issue citations to non-licensees before taking any other type of action sometimes hinders us in our investigations, and allows targets to disappear before we are in a position to take action against them. Eliminating the citation requirement in section 503(b) of the Act would enable more streamlined enforcement. In addition, I believe that raising maximum forfeiture penalties, currently prescribed by statute, would assist the Commission in taking effective enforcement action, as well as act as a deterrent to companies who otherwise view our current forfeiture amounts simply as costs of doing business. Further, the one-year statute of limitations in section 503 of the Communications Act for bringing action has been a source of difficulty at times. In particular, when the violation is not immediately apparent, or when the Commission undertakes a complicated investigation, we often run up against the statute of limitations and must compromise our investigation, or begin losing violations for which we can take action.

Conclusion

The disclosure of consumers' private calling records is a significant privacy invasion. The Commission is taking numerous steps to try to address practice as soon as possible. I look forward to working collaboratively with the members of this Committee, other Members of Congress, as well as my colleagues at the Commission and at the Federal Trade Commission to ensure that consumers' personal phone data remains confidential. Thank you for the opportunity to testify, and I would be pleased to respond to your questions.